

PATENT

Atty Docket No.: 10002170-2
App. Scr. No.: 09/726,072

IN THE CLAIMS:

Please find below a listing of all of the pending claims. The statuses of the claims are set forth in parentheses.

1. (Currently Amended) A secure network configured to carry data, comprising:

a plurality of network bubbles, each network bubble having a plurality of bubble partitions, each bubble partition having at least one network device configured to transmit and receive data, and

all of the network devices corresponding to the same respective network bubble having unrestricted network access with each other and the same network security policy that controls data movement between the network devices of different network bubbles; [[and]]

a network control point having one or more network control point devices, a first network device of a first network bubble being connected to the network control point through at least one network control point device and a second network device of a second network bubble being connected to the network control point through at least one network control point device wherein the network control point applies the security policy of the first network bubble to data for the first network device and the security policy of the second network bubble to data for the second network device, wherein the security policy of the first network bubble is distinct from the security policy of the second network bubble; and

an inter-bubble device connecting the first and second network bubbles to one another and enforcing the network security policy of the first and second network bubbles.

2. (Canceled).

PATENT

Atty Docket No.: 10002170-2
App. Ser. No.: 09/726,072

3. (Original) A secure network as defined in claim 1, wherein each of the plurality of bubble partitions that belong to the same bubble has the same network security policy applied at each of the plurality of network control points that are connected to the plurality of bubble partitions.
4. (Original) A secure network as defined in claim 1, wherein each of the plurality of bubble partitions has unrestricted network connectivity to all other bubble partitions within the same bubble.
5. (Original) A secure network as defined in claim 1, wherein each of the plurality of bubble partitions is defined by an address range.
6. (Original) A secure network as defined in claim 5, wherein each of the network devices in each of the plurality of bubble partitions has an address contained within the address range.
7. (Original) A secure network as defined in claim 6, wherein each address exists in only one of the plurality of bubble partitions.
8. (Original) A secure network as defined in claim 1, wherein each of the plurality of network control points ensures source address integrity at each bubble boundary.

PATENT

Atty Docket No.: 10002170-2

App. Ser. No.: 09/726,072

9. (Original) A secure network as defined in claim 1, wherein each of the plurality of bubble partitions is connected to at least two network control point devices to achieve high availability in the case of a failed interface or network control point device.
10. (Original) A secure network as defined in claim 1, wherein data may be transmitted between two network devices in different bubble partitions of the same network bubble without restriction by the network bubble boundaries.
11. (Original) A secure network as defined in claim 1, wherein the plurality of network control points are coupled to one another and form a virtual backbone that is external to all of the plurality of network bubbles.
12. (Original) A secure network as defined in claim 11, wherein each of the plurality of network control points ensure source address integrity across the virtual backbone.
13. (Original) A secure network as defined in claim 1, wherein each network device connects to only one network control point.
14. (Original) A secure network as defined in claim 1, wherein the total number of network control points is greater than the number of network control points connected to any one particular bubble partition.

PATENT

Atty Docket No.: 10002170-2

App. Ser. No.: 09/726,072

15. (Original) A secure network as defined in claim 1, wherein all data transmitted from one network device to another network device traverses only one network control point.

16. (Original) A secure network as defined in claim 1, wherein all data transmitted from one network device to another network device traverses only two network control points.

17. (Currently Amended) A secure network configured to transmit data, comprising:
a first and a second network bubble, each network bubble having a distinct network security policy and a plurality of bubble partitions, each bubble partition having a plurality of network devices having unrestricted network access with each other and configured to transmit and receive data; [[and]]

a network control point having one or more network control point devices, a first network device of the first network bubble being connected to the network control point to which a second network device of the second bubble is also connected, wherein the network control point device applies the distinct security policy of the first bubble to data for the first network device and the distinct security policy of the second bubble to data for the second network device to control movement of data between the first and a second network bubble;
and

an inter-bubble device connecting the first and a second network bubble to one another and enforcing the network security policy of the first and a second network bubble.

PATENT

Atty Docket No.: 10002170-2

App. Ser. No.: 09/726,072

18. (Original) A secure network as defined in claim 17, wherein all data transmitted from one network device in the first network bubble to another network device in the second network bubble traverses only one network control point.

19. (Original) A secure network as defined in claim 17, wherein all data transmitted from one network device in the first network bubble to another network device in the second network bubble traverses only two network control points.

20. (Original) A secure network as defined in claim 17, wherein all data transmitted from one network device in the first network bubble to another network device in the second network bubble traverses more than two network control points.

21. (Original) A secure network as defined in claim 17, wherein the network control point enforces source integrity for all bubble partitions that are connected to it.

22. (Original) A secure network as defined in claim 17, wherein each bubble partition connects to only one network control point.

23. (Canceled).

24. (Original) A secure network as defined in claim 17, wherein each of the plurality of bubble partitions that belong to the same bubble has the same network security policy applied

PATENT

Atty Docket No.: 10002170-2
App. Ser. No.: 09/726,072

at each of the plurality of network control points that are connected to the plurality of bubble partitions.

25. (Original) A secure network as defined in claim 17, wherein each of the plurality of bubble partitions has unrestricted network connectivity to all other bubble partitions within the same network bubble.

26. (Original) A secure network as defined in claim 17, wherein each of the plurality of bubble partitions is connected to at least two network control point devices to achieve high availability in the case of a failed interface or network control point device.

27. (Original) A secure network as defined in claim 17, wherein each of the plurality of bubble partitions is defined by an address range.

28. (Original) A secure network as defined in claim 27, wherein each of the plurality of network devices in each of the plurality of bubble partitions has an address contained within the address range.

29. (Original) A secure network as defined in claim 28, wherein each address exists in only one of the plurality of bubble partitions.

PATENT

Atty Docket No.: 10002170-2
App. Scr. No.: 09/726,072

30. (Original) A secure network as defined in claim 17, wherein data may be transmitted between two network control point devices in different bubble partitions of the same network bubble without restriction by the plurality of network control points.

31. (Original) A secure network as defined in claim 17, wherein the plurality of network control points are coupled to one another and form a virtual backbone that is external to the first and the second network bubble.

32. (Original) A secure network as defined in claim 31, wherein each of the plurality of network control points ensure source address integrity across the virtual backbone.

33. (Currently Amended) A secure network as defined in claim 17, ~~further comprising an~~ wherein the interbubble device is connected to the first network bubble and the second network bubble without being connected to the plurality of network control points and configured to enforce the network security policy of the first and the second network bubble.

Claims 34-47. (Canceled).

48. (Currently Amended) The secure network as defined in claim 1 wherein at least two of the plurality of bubble partitions associated with the first network bubble are in different geographic locations, wherein each partition connects to a different network control point device which enforces the security policy of the first network bubble for the devices in the respective partition.

PATENT**Atty Docket No.: 10002170-2**
App. Ser. No.: 09/726,072

49. (New) The secure network as defined in claim 1 wherein the inter-bubble device applies the network security policy of both the first network bubble and the second network bubble to move data between the first and second network bubbles.